Możliwość dofinansowania

NTG.pl Sp. z o.o.

4,4 / 5

5 471 ocen

Szkolenie wieczorowe: Wstęp do Ethical Hackingu – Cyberzagrożenia i Bezpieczna Praca

Numer usługi 2025/08/29/5395/2971247

zdalna w czasie rzeczywistym

Usługa szkoleniowa

4 h

03.10.2025 do 03.10.2025

400,00 PLN brutto

400,00 PLN netto

100,00 PLN brutto/h

100,00 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Nowy start w Małopolsce z EURESEM, Zachodniopomorskie Bony Szkoleniowe, Małopolski Pociąg do kariery
Grupa docelowa usługi	Szkolenie Ethical Hacking – poziom średniozaawansowany jest przeznaczone dla osób, które posiadają podstawową wiedzę z zakresu cyberbezpieczeństwa i chcą rozwinąć umiejętności w praktycznym testowaniu zabezpieczeń. W szczególności szkolenie jest skierowane do: • administratorów sieci i systemów, którzy chcą lepiej chronić swoją infrastrukturę IT, • początkujących pentesterów, szukających praktycznych umiejętności i doświadczenia, • studentów kierunków informatycznych, zainteresowanych bezpieczeństwem IT, • pasjonatów cyberbezpieczeństwa, którzy chcą pogłębić swoją wiedzę w zakresie testów penetracyjnych i ataków na usługi sieciowe oraz aplikacje webowe.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	30-09-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	4

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestnika do rozpoznawanie najczęstszych zagrożeń cyberbezpieczeństwa (phishing, malware, ataki na hasła, fałszywe strony) oraz stosowania dobrych praktyk ochrony danych i kont w pracy i życiu prywatnym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozróżnia pojęcia haker, cracker, ethical hacker. Uczestnik wskazuje cechy wiadomości phishingowej.	Uczestnik wskazuje elementy fałszywego e-maila.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik zna rodzaje złośliwego oprogramowania i sposoby infekcji. Uczestnik zna zasady utworzenia silnego hasła i rozumie rolę 2FA	Uczestnik dopasowuje przykłady (np. ransomware, spyware) do definicji. Zna zasady tworzenia hasła spełniającego kryteria długości i złożoności.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik rozpoznaje fałszywe linki logowania i sprawdza certyfikat SSL.	Uczestnik wskazuje podejrzane elementy strony.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik stosuje zasady bezpiecznej pracy zdalnej (VPN, przechowywanie danych).	Uczestnik podaje właściwe kroki konfiguracji lub zabezpieczenia danych.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie realizowane w godzinach dydaktycznych.

📘 Jak wygląda szkolenie?

Szkolenie prowadzone jest w sposób uporządkowany i praktyczny - składa się z trzech etapów:

- - Wprowadzenie teoretyczne
  - Ćwiczenia wspólne z trenerem – wykonujemy zadania krok po kroku, ucząc się na konkretnych przykładach.
  - Zadania do samodzielnego wykonania – utrwalenie wiedzy.

🤝 Opieka poszkoleniowa

Po zakończeniu szkolenia zapewniamy pełną opiekę poszkoleniową:

- - kontakt z trenerem
  - wsparcie techniczne i merytoryczne po szkoleniu
  - dodatkowe materiały i wskazówki, które pomogą wracać do kluczowych zagadnień.

✅ Program szkolenia:

Moduł 1: Kim jest haker?

Omówione zostaną tematy:

- Różnice: haker, cracker, ethical hacker
- Motywacje atakujących
- Cykl ataku (rekonesans → eksploitacja → eskalacja → utrzymanie dostępu)
- Czym jest test penetracyjny?

Moduł 2: Jak działa phishing i socjotechnika?

Poznasz:

- Rodzaje phishingu: e-mail, SMS, telefon, linki
- Typowe cechy fałszywych wiadomości
- 5 zasad bezpiecznego e-maila
- Ćwiczenie: analiza przykładowego phishingu

Moduł 3: Złośliwe oprogramowanie – jak się przed nim chronić?

Będziesz wiedział jak się chronić i wprowadzimy cię do wiedzy jak tworzyć:

- Malware: wirusy, ransomware, spyware
- Drogi infekcji: dokumenty, pendrive'y, strony WWW
- Case study: atak ransomware w firmie
- Dobre praktyki: praca z plikami i załącznikami

Moduł 4: Bezpieczne hasła i uwierzytelnianie

Zgłębisz wiedzę na temat haseł:

- Jak łamane są hasła: brute-force, słowniki, wycieki
- Jak tworzyć silne hasła?
- Menedżery haseł – przegląd i rekomendacje
- Czym jest 2FA i jak działa
- Ćwiczenie: testy na HaveIBeenPwned

Moduł 5: Ataki przez strony internetowe

Zaznajomisz się z technikami dotyczącymi stron internetowych ucząc się o:

- Fałszywe strony logowania – jak je rozpoznać
- MITM – przechwytywanie danych na Wi-Fi
- Rola certyfikatów SSL i jak je sprawdzać

- Ćwiczenie: analiza fałszywego loginu

Moduł 6: Praca zdalna i bezpieczeństwo danych

Dowiesz się również o bezpieczeństwie pracy zdalnej:

- Zagrożenia pracy poza biurem
- Rola VPN i jego poprawna konfiguracja
- Jak bezpiecznie przechowywać dane firmowe i osobowe

Moduł 7: Co robić po incydencie?

Zgłaszanie incydentów i wstęp do Blue Teamu:

- Jak zgłosić incydent w firmie
- Co robić, a czego unikać po ataku
- Znaczenie szybkiej reakcji i komunikacji

Test z wynikiem generowanym automatycznie.

Harmonogram

Liczba przedmiotów/zajęć: 4

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 4 Moduł 1: Kim jest haker? Moduł 2: Jak działa phishing i socjotechnika? Moduł 3: Złośliwe oprogramowanie – jak się przed nim chronić?	Daniel Gawryś	03-10-2025	17:00	18:30	01:30
2 z 4 Przerwa - nie wlicza się w czas usługi	Daniel Gawryś	03-10-2025	18:30	18:45	00:15
3 z 4 Moduł 4: Bezpieczne hasła i uwierzytelnianie Moduł 5: Ataki przez strony internetowe Moduł 6: Praca zdalna i bezpieczeństwo danych Moduł 7: Co robić po incydencie?	Daniel Gawryś	03-10-2025	18:45	20:00	01:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 4 Test z wynikiem generowanym automatycznie	Daniel Gawryś	03-10-2025	20:00	20:15	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	400,00 PLN
Koszt przypadający na 1 uczestnika netto	400,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Daniel Gawryś

Entuzjasta cyberbezpieczeństwa z praktycznym doświadczeniem w przeprowadzaniu szkoleń, testów penetracyjnych, analizie podatności i zabezpieczaniu środowisk IT(Trener posiada doświadczenie zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR)
Posiadam certyfikaty eCPPT, CPTS
(od HTB), Cisco Junior Cybersecurity Analyst i Cisco Certified Ethical Hacker. Tworzy własne narzędzia w Pythonie i Bashu, aktywnie uczestniczę w CTF-ach oraz rozwija umiejętności w homelabach zgodnie z metodykami OWASP i MITRE ATT&CK. Prowadzący posiada wiedzę i doświadczenie z zakresu zaawansowanych technik hackingu oraz przeciwdziałania atakom. Posiada doświadczenie zdobyte w oparciu o przeprowadzone pentest infrastruktury sieci szkolnej, sieci w placówkach państwowych oraz stron internetowych różnych firm.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Autorskie materiały szkoleniowe w wersji elektronicznej.

Informacje dodatkowe

Po ukończeniu szkolenia uczestnik otrzymuje certyfikat potwierdzający zdobyte umiejętności.

Jak skorzystać z usług dofinansowanych?

- Krok 1: Założenie konta indywidualnego/instytucjonalnego w Bazie Usług Rozwojowych.
- Krok 2: Złożenie wniosku do Operatora, który rozdziela środki w Twoim województwie.
- Krok 3: Uzyskanie dofinasowania.
- Krok 4: Zapisanie na szkolenie poprzez platformę BUR.

Podczas szkoleń istnieje możliwość przeprowadzenia kontroli/audytu usługi przez osoby do tego upoważnione przez PARP.

Dlaczego wybrać firmę NTG Sp. z o.o.?

- Realizujemy szkolenia od 2002 roku.
- Mamy wyspecjalizowaną kadrę szkoleniową.
- Przeprowadzimy Ciebie przez cały proces pozyskania dofinansowania.
- Bezpłatnie pomożemy w uzyskaniu dofinansowania.
- Zaproponujemy szkolenia dopasowane do potrzeb Twojej firmy.
- Dostarczymy dokumentację szkoleniową, niezbędną do rozliczenia.
- Odpowiemy na wszystkie Twoje pytania.

Warunki techniczne

Zalecamy korzystanie z dodatkowego monitora, aby móc swobodnie wykonywać ćwiczenia wraz z trenerem.

Szkolenie będzie realizowane za pośrednictwem aplikacji Microsoft Teams (nie jest wymagana instalacja aplikacji). Link do spotkania można otworzyć za pomocą przeglądarki i jest aktywny podczas trwania usługi.

Do poprawnego udziału w usłudze uczestnik powinien posiadać komputer z kamerą, mikrofonem, dostępem do Internetu; szybkością pobierania i przesyłania 500 kb/s; aktualną wersje przeglądarki Microsoft Edge, Internet Explorer, Safari lub Chrome. Zalecamy posiadanie systemu operacyjnego Windows 10 oraz min. 2 GB RAM pamięci.

Kontakt

NTG.pl Sp. z o.o.

E-mail ntg@ntg.edu.pl
Telefon (+48) 609 009 742